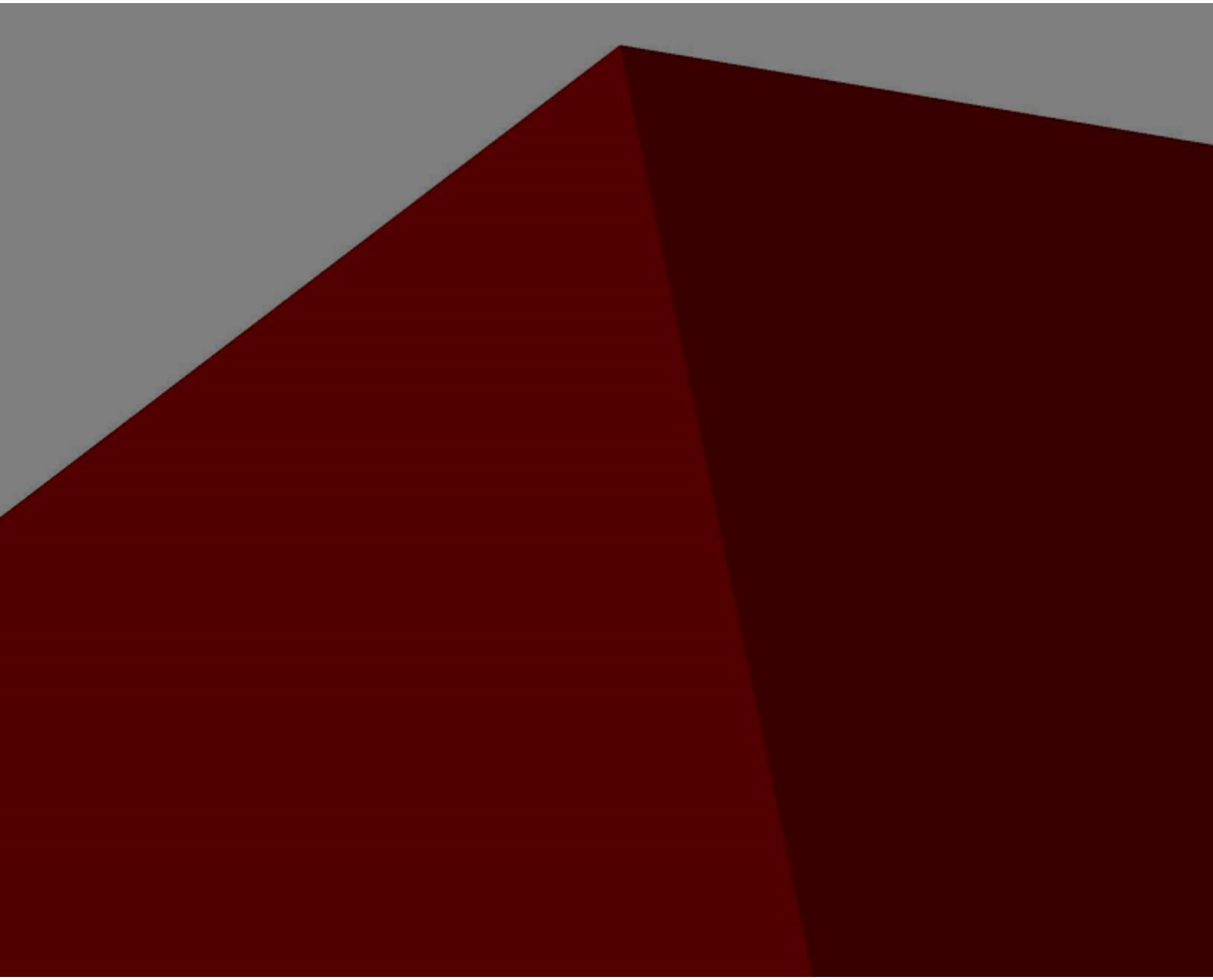
Конкурсное задание

Компетенция

Сетевое и системное администрирование 14-16

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Задание
4. Критерии оценки



Количество часов на выполнение задания: 8 ч. Версия 1.2 от 02.03.2021

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Командный зачёт, 2 человека в команде.

2. ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

ВВЕДЕНИЕ

Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем в сфере интеграции и аутсорсинга домашних и корпоративных вычислительных сетей. Если вы можете выполнить задание с высоким результатом, то вы сможете достаточно успешно обслуживать информационную инфраструктуру небольшого предприятия, ну, или хотя бы делать вид.

Данное конкурсное задание разработано с использованием различных технологий, совместное использование которых представляет собой достаточно сложную инфраструктуру. Требования в задании представлены в общем виде, конкретный метод выполнения и технологии, необходимые для его реализации, вы вправе выбрать самостоятельно с учётом указанных в задании требований.

Некоторые технологии должны работать в связке или поверх других. Например, динамическая маршрутизация выполняется поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает что работа не будет оценена. Например, для удаленного доступа необходимо настроить IPsec-туннель, внутри которого организовать GRE-туннель. Если вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа. Главной задачей является получение работоспособной системы в том или ином виде, а также её ежедневная доработка и улучшение.

СХЕМА ОЦЕНКИ

Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен только один раз и повторная оценка данного аспекта проводится не будет.

Следует также учесть, что для данного задания возможна автоматическая оценка результатов.

Процедура оценки результатов выполнения задания будет производиться после полного

выполнения задания по окончании второго дня соревнований.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Конкурсное задание выполнимо в полном объеме с привлечением оборудования и материалов, указанных в Инфраструктурном листе.

Для выполнения задания возможно использовать виртуальную инфраструктуру. Рекомендуемые версии ПО: Debian 10, Windows Server 2019 Standard, Windows 10 Enterprise, OpenWRT 18.06, OPNSense 19.7, VyOS 1.3.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь рекомендуется прочитать задание полностью. Следует обратить внимание, что задание составлено не в строгом хронологическом порядке. Для выполнения некоторых пунктов задания может потребоваться выполнение действий из других пунктов, которые изложены в задании ниже. Таким образом, порядок выполнения задания и распределение временных затрат определяется участниками самостоятельно.

Конкурсное задание имеет сквозную структуру, и предполагается, что вы продолжаете его выполнение во второй и последующие дни с того момента, на котором остановились в предыдущий. Вам доступно полное задание на все конкурсные дни.

Рекомендуется тщательно проверять результаты своей работы. Также учтите, что в конце каждого дня вам необходимо по указанию экспертов и в их присутствии выключить все виртуальные машины, а затем включить их в желаемом порядке. Также рабочее место может быть выключено в ночное время.

Виртуальные машины могут иметь предустановленное программное обеспечение, которое будет применяться при проверке и оценке, его не рекомендуется удалять.

Доступ ко всем виртуальным Linux-машинам настроен по аккаунту **root** с паролем **toor**.

При первом доступе к Windows-машинам следуйте инструкциям мастера.

Если Вам требуется установить пароль, не указанный в задании, а также в инструкциях и файлах дополнений, используйте: **P@ssw0rd**

3. ЗАДАНИЕ

ПРЕДНАСТРОЙКИ РАБОЧЕГО МЕСТА

Для связи с интернет провайдером используйте следующие настройки:

Устройство	Адрес IPv4/Маска	Шлюз
HomeRTR	178.207.179.6/29	178.207.179.1
ExtClient	77.34.141.141/22	77.34.140.1
FW1	62.33.111.34/29	62.33.111.33/29

ТАБЛИЦА 1. НАСТРОЙКИ IP-АДРЕСАЦИИ

Устройство	Интерфейс	Адрес IPv4/Маска
FW1	внешний	62.33.111.34/29
	в сторону R1	172.16.1.1/30
	в сторону R2	172.16.2.1/30
R1	в сторону FW1	172.16.1.2/30
	в сторону R2	172.16.0.1/30
	Сеть Server_Network	10.1.10.254/24
	Сеть Lin_Network	10.2.20.254/24
R2	в сторону FW1	172.16.2.2/30
	в сторону R1	172.16.0.2/30
	Сеть Server_Network	10.1.10.253/24
	Сеть Win_Network	10.1.20.254/24
WinServer	Сеть Server_Network	10.1.10.100/24
WinClient1	Сеть Win_Network	DHCP

WDSClient	Сеть Win_Network	DHCP
WebServer	Сеть Server_Network	10.1.10.200/24
LinClient	Сеть Lin_Network	DHCP
Устройство	**Интерфейс**	**Адрес IPv4/Маска**
HomeRTR	внешний	178.207.179.6/29
	внутренний	192.168.0.1/24
HomeLaptop		DHCP
HomePC		DHCP
HomeServer		DHCP (Static lease)

ЗАДАЧИ И ТЕХНОЛОГИИ, РАБОТОСПОСОБНОСТЬ КОТОРЫХ ПРОВЕРЯЕТСЯ В ЗАДАНИИ

Базовая настройка

1. Настройте имена всех устройств и виртуальных машин в соответствии с топологией.
2. Настройте IPv4-адресацию локальных сетей в соответствии с **Таблицей 1**.
3. IP-адреса для связи с интернет провайдерами указаны в разделе "Преднастройки рабочего места"

Настройка сети домашнего офиса

1. Обеспечьте связь всех устройств внутри локальной сети домашнего офиса, а также доступ в интернет для всех пользователей.
    a. Для частных адресов необходимо настроить NAT.
    b. Для проверки доступа к сети интернет можно использовать адрес worldskills.ru.
2. В качестве DHCP сервера используйте **HomeRTR**.
    a. Используйте пул адресов 192.168.0.100-192.168.0.200.
    b. В качестве адреса DNS сервера используйте адрес **HomeRTR**.
3. Настройте пересылку на DNS-сервер провайдера.
    a. Включите на **HomeRTR** пересылку DNS-запросов из локальной сети на DNS-сервер 1.1.1.1.

Настройка сети компании Sunshine, LLC

1. Настройте доступ в Интернет для всех устройств центрального офиса.
    a. Настройте адреса на всех сетевых интерфейсах согласно Таблице 1.
    b. На межсетевом экране FW1 настройте NAT для всех сетей центрального офиса.
    c. Сделайте дополнительные настройки маршрутизации, необходимые для обеспечения доступа клиентов в Интернет.
2. На маршрутизаторах R1 и R2 настройте удаленный доступ по протоколу SSH.
    a. Разрешите доступ для пользователя **netadmin** с паролем **netpass**
    b. Запретите подключение с учетной записью по умолчанию.
3. На виртуальной машине WinServer предустановлен Windows Server 2019 Standard.
4. Сделайте следующую базовую конфигурацию **WinServer**:
    a. Раскладка клавиатуры по умолчанию 'US'.
    b. Имя машины должно соответствовать схеме сети.
    c. Сервер должен отвечать на запросы по протоколу ICMP.
    d. Установите роль контроллера домена **sunshine.local** с максимально возможным режимом работы леса.
5. **WinServer** должен выполнять роль DNS сервера.
    a. Настройте необходимые зоны прямого и обратного просмотра.

b. Все неизвестные запросы сервер должен переадресовывать на адрес 1.1.1.1

6. Настройте автоконфигурацию адресов для всех клиентов в домене:
   a. Имя зоны: **Win_Network**;
      i. Диапазон адресов: 10.1.20.90 - 99;
      ii. Маска: 24;
      iii. Шлюз: 10.1.20.254;
      iv. DNS: 10.1.10.100.
   b. Имя зоны: **Lin_Network**;
      i. Диапазон адресов: 10.2.20.90 - 99;
      ii. Маска: 24;
      iii. Шлюз: 10.2.20.254;
      iv. DNS: 10.1.10.100.
7. Компьютеры клиентов должны получать адрес с центрального DHCP сервера **WinServer**. Настройте оборудование таким образом, чтобы клиенты из **Win_Network** и **Lin_Network** могли получать информацию с этого DHCP сервера.
8. На виртуальной машине **WinClient1** предустановлена ОС Windows 10 Enterprise. Выполните на этой машине следующую настройку:
   a. Раскладка клавиатуры по умолчанию 'US'.
   b. Имя машины должно соответствовать схеме сети.
   c. Машина должна отвечать на запросы по протоколу ICMP.
   d. Введите машину в домен **sunshine.local**.
9. На виртуальных машинах **HomeLaptop** и **HomePC** также предустановлена ОС Windows 10 Enterprise. Выполните на этих машинах следующую настройку:
   a. Раскладка клавиатуры по умолчанию 'US'.
   b. Имя машин должно соответствовать схеме сети.
   c. Машины должна отвечать на запросы по протоколу ICMP.
   d. Машины должны быть членами рабочей группы **HomeNet**.
10. На всех машина с ОС Windows 10 Enterprise должна быть активна только одна локальная пользовательская учетная запись **Administrator/P@ssw0rd.**

Настройка сети домашнего офиса

1. Настройте **HomeServer** в качестве сервера хранения данных.
   a. Сервер должен получать адрес по DHCP от **HomeRTR**. Настройте DHCP-сервер таким образом, чтобы это был всегда один и тот же адрес..
   b. Настройте службу FTP.
      i. Используйте каталог для хранения данных /opt/storage.
      ii. Запретите анонимный доступ.
      iii. Пользователь **ftpuser** с паролем **ftppass** должен обладать правами на чтение и запись.

c. Настройте службу Samba для организации общего доступа к файлам и папкам для **HomeLaptop** и **HomePC**.
   i. Используйте каталог для хранения данных /opt/storage.
   ii. Каталог /opt/storage должен автоматически подключаться на устройствах **HomeLaptop** и **HomePC** в качестве сетевого диска Z:\.
   iii. Доступ к диску Z:\ должен быть предоставлен на чтение и запись.
   iv. Доступ должен быть предоставлен пользователю **smbuser** с паролем **smbpass**.
   v. Анонимный доступ к ресурсу должен быть запрещен.

2. Обеспечьте внешнее подключение к службе FTP.
   a. Виртуальная машина **ExtClient** должна иметь возможность подключаться к службе FTP с использованием логина и пароля.
   b. Обеспечьте доступ на чтение и запись.
   c. Для подключения должен использоваться внешний IPv4 адрес **HomeRTR**.
3. На виртуальной машине **HomePC**.
   a. Создайте пользователя **Home1**.
   b. Создайте папку **Photos**.
4. На виртуальной машине **HomeLaptop**.
   a. Создайте пользователя **Home2**.
   b. Создайте папку **Videos**.
5. Пользователи **Home1** и **Home2** должны иметь доступ по сети к папкам **Photos** и **Videos**.
   a. Пользователь **Home1** должен иметь возможность просматривать, редактировать и удалять файлы в обеих папках.
   b. Пользователь **Home2** должен иметь возможность только просматривать файлы в обеих папках.

Настройка сети компании Sunshine, LLC

1. Включите на всех устройствах сетевое обнаружение с помощью протокола LLDP.
2. Настройте маршрутизацию между FW1, R1 и R2 с помощью OSPFv2.
   a. Используйте нулевую область.
   b. R1 и R2 должны анонсировать в OSPF все локальные сети.
   c. R1 и R2 должны использовать маршрут по умолчанию, который они получают по OSPF от FW1.
   d. R1 и R2 не должны посылать hello-пакеты в сторону серверов и клиентов.
3. Виртуальная машина **WebServer** должна выполнять роль веб-сервера.
   a. Используйте путь /opt/html в качестве корневого каталога сайта.
   b. Создайте файл с именем index.html со следующим содержанием:

```
<html><body>
<h1>Welcome to Sunshine Web Server!</h1>
```

</body></html>

c. Используйте файл index.html в качестве главной страницы сайта.
d. Доступ к сайту должен осуществляться по протоколу http.
e. Для доступа к сайту должно быть настроено доменное имя **web.sunshine.local**.

4. Виртуальная машина **LinClient** должна получать IPv4 автоматически по протоколу DHCP.
5. Обеспечьте доступ к **WebServer** по протоколу ssh.
   a. Должна использоваться учетная запись **sshuser** с паролем **sshpass**.
   b. После аутентификации пользователь **sshuser** должен иметь возможность повысить уровень привилегий с помощью команды sudo без ввода пароля.
6. На виртуальной машине **LinClient** установите графическую рабочую среду.
   a. Используйте графическую среду MATE или GNOME.
   b. Настройте runlevel так, чтобы графическая среда загружалась автоматически при перезагрузке.
7. В домене **sunshine.local** создайте следующие подразделения:
   a. Corp;
   b. Corp\Office;
   c. Corp\Sales;
   d. Corp\ITAdmin.
8. В соответствующих подразделениях создайте глобальные группы безопасности **G_Office**, **G_ITAdmin** и **G_Sales**.
9. В подразделении **Sales** создайте пользователей **sa_user1** и **sa_user2**. Пользователи не должны иметь возможности менять свой пароль и должны быть членами группы **G_Sales**. Пользователь **sa_user2** может аутентифицироваться на компьютерах только между 8-00 и 14-00 с понедельника по субботу.
10. В подразделении **ITAdmin** создайте пользователей: **NetAdmin**, **OpenSource** и **SMAdmin**. **SMAdmin** должен быть членом группы **Domain Admins**. **NetAdmin** и **OpenSource** должны быть членами группы **G_ITAdmin** .
11. В подразделении **Office** создайте пользователя **of_user**. Переместите учетную запись компьютера **WinClient1** в подразделение **Office**.
12. На контроллере домена создайте общую папку **Homes**. Домашние директории всех пользовательских учетных записей должны располагаться в данной папке и быть доступны пользователям как сетевой диск с буквой H. При обращении к папке **Homes** по сети пользователи должны иметь доступ только к своему каталогу.

Настройка сети домашнего офиса

1. Настройте защищённое соединение с помощью протокола IPsec между маршрутизатором **HomeRTR** и межсетевым экраном **FW1**.
   a. Необходимо обеспечить связь между устройствами домашней сети и серверами в сети Server Network.
   b. Используйте аутентификацию по общему ключу.

c. Используйте для защиты данных шифрование AES с длиной ключа 256 и алгоритм хэширования SHA-256.

2. Сделайте дополнительные настройки безопасности для **HomeRTR**.
   a. Запретите доступ со стороны сети Интернет на внешнем интерфейсе ко всем службам, кроме FTP и IPsec.
   b. При этом у пользователей локальной сети должен оставаться доступ в Интернет.

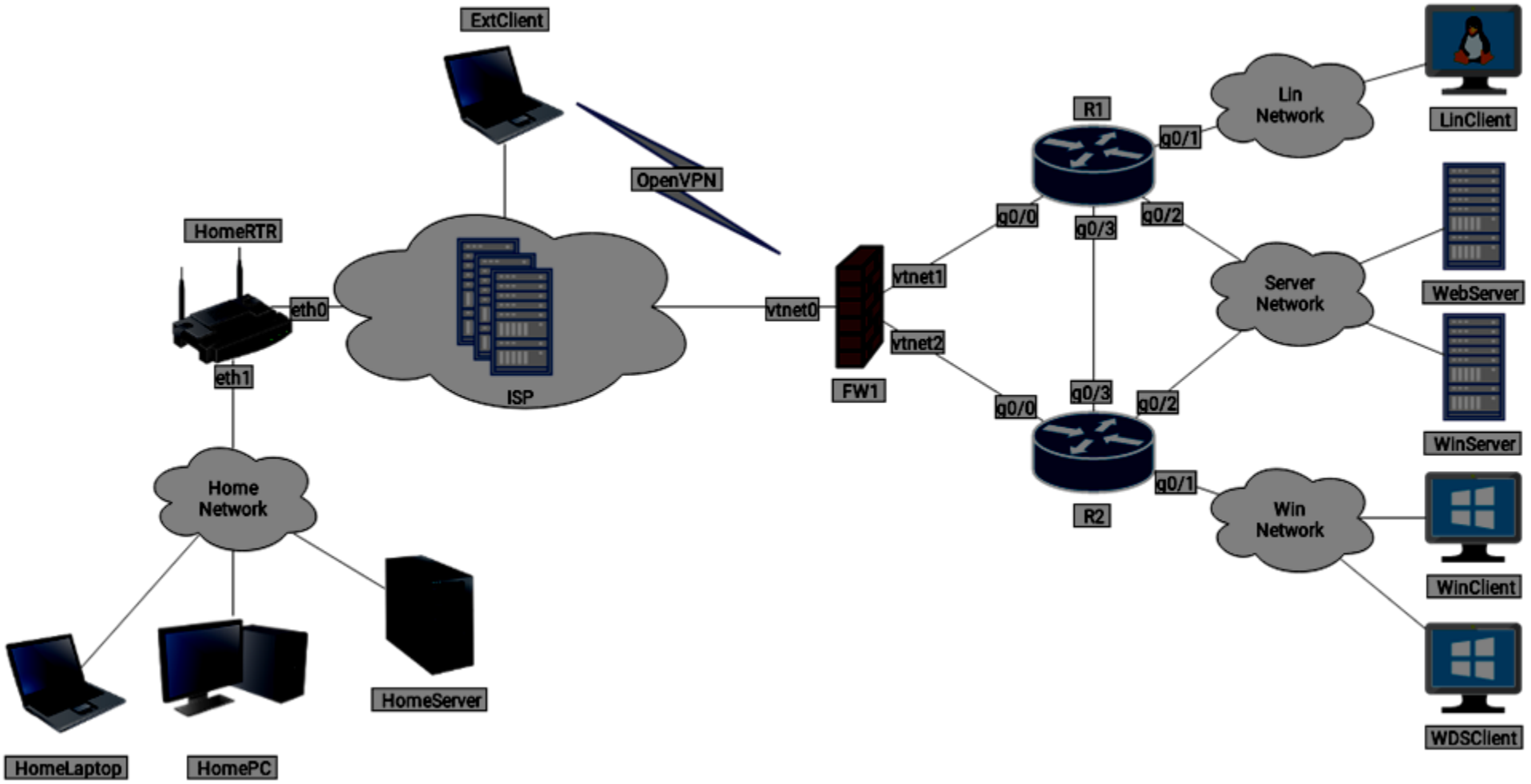
Настройка сети компании Sunshine, LLC

1. Настройте доступ к **WebServer** по протоколу https.
   a. При обращении к сайту по протоколу http должна происходить автоматическая переадресация на протокол https.
   b. Обеспечение отсутствия предупреждающих сообщений о недоверенном соединении не требуется.
2. Настройте внешний доступ к сайту на **WebServer**.
   a. Доступ должен быть предоставлен по внешнему IPv4 адресу **FW1**.
3. На виртуальной машине **WebServer** создайте swap-файл.
   a. Объем файла 200 МБайт.
   b. Файл должен использоваться как swap.
   c. swap-файл должен автоматически монтироваться при перезагрузке.
4. Настройте для сети Server Network резервирование шлюза с помощью VRRP
   a. Используйте адрес 10.1.10.254.
   b. Используйте номер группы 10.
   c. В качестве шлюза должен выступать **R2**, в случае его отказа должно происходить переключение на **R1**.
5. Виртуальная машина **ExtClient** должна иметь возможность устанавливать VPN соединение с **FW1**.
   a. Установите и настройте клиент OpenVPN.
   b. После установления VPN соединения локальные сайты компании должны быть доступны по доменному имени. Для проверки используйте имя **web.sunshine.local**.
   c. VPN соединение должно устанавливаться при вызове скрипта startvpn.sh.
   d. VPN соединение должно разрываться при вызове скрипта stopvpn.sh.
   e. Скрипты startvpn.sh и stopvpn.sh не должны требовать ввода дополнительных параметров и устанавливать или разрывать соединение без участия пользователей.
   f. Для хранения файлов скриптов startvpn.sh и stopvpn.sh используйте каталог /opt/scripts.
6. В домене **sunshine.local** создайте групповые политики и примените их к определенным подразделениям:
   a. Имя GPO: **Office GPO**. Подразделение: **Office**. Настройка: пользователи не могут менять экран блокировки на компьютерах этого подразделения.

b. Имя GPO: **Sales GPO**. Подразделение: **Sales**. Настройка: пользователи не должны иметь доступ к командной строке.
c. Имя GPO: **Corp**. Подразделение: **Corp**. Настройка: У пользователей с рабочего стола удалена Корзина.
d. Имя GPO: **Local admin**. Подразделение: **ITAdmin**. Настройка: члены группы **G_ITAdmin** должны быть членами локальной группы Администраторы на всех клиентах домена.
e. Имя GPO: **Default domain policy**. Настройка: Запрещена приветственная анимация при первом входе пользователя на клиентский компьютер домена.

7. На машинах **HomePC** и **HomeLaptop** запретите пользователям устанавливать пароли короче 5 символов.
8. На машине **WinServer** установите Windows Deployment System. В качестве образа ОС для установки используйте доступный ISO с Windows 10 Enterprise. При необходимости используйте для хранения образа жесткий диск объемом 15Gb. Обеспечьте согласованную работу WDS и DHCP в сетевом сегменте. Система должна отвечать на запросы любых компьютеров. Установка ОС на компьютеры после их включения должна начинаться без участия пользователя. Устанавливать ОС может только администратор домена **sunshine.local**.
9. Установите на машину **WDSClient** операционную систему с помощью Windows Deployment System. Система автоматически должна ввести рабочую станцию в домен **sunshine.local** с именем **WinClient2**.

4. ТОПОЛОГИЯ


ExtClient
OpenVPN
HomeRTR
eth0
eth1
ISP
vtnet0
FW1
vtnet1
vtnet2
R1
R2
g0/0
g0/1
g0/2
g0/3
Lin Network
LinClient
Server Network
WebServer
WinServer
Win Network
WinClient
WDSClient
Home Network
HomeServer
HomeLaptop
HomePC